OFDM BASED LOW POWER SECURED COMMUNICATION USING AES WITH VEDIC MATHEMATICS TECHNIQUE FOR MILITARY APPLICATIONS

Elakkiya.V[1], Sharmila.S[2], Swathi Priya A.S[3], Vinodha.K[4]

[1,2,3,4]Department of Electronics and Communication Engineering, Saranathan College of Engineering, Trichy, INDIA

ABSTRACT- The main objective of this paper is to design and implement the AES algorithm with Vedic Mathematics technique by adopting OFDM to avoid trapping the data by attackers during secure communication, especially for military applications. This paper depicts the high level implementation of AES algorithm with encryption and decryption process in which Vedic Mathematics is employed in Mix Columns followed by modulation technique. The technique involved in modulation is QPSK in order to achieve high throughput. The OFDM also consists of Radix 2 ,16 point IFFT and FFT technique. The design has been coded in Verilog and targeted into Xilinx Spartan 3 FPGAs. For hardware implementation, we prefer FPGA due to its reconfiguration nature, low price and marketing speed .The novelty of this paper is Vedic Mathematics which accomplish low power consumption.

Index Terms- AES, Vedic Mathematics, OFDM, QPSK, Radix 2 IFFT & FFT

I. INTRODUCTION

Military organizations are concerned about the security of information exchanges. A reliable system for such message exchanges is considered to be a particular strength for such organizations. Data security is an essential objective for the military and diplomatic services which have many commercial uses and applications such as electronic banking, electronic mail, internet network service, messaging networks etc. Security is the most important part in data communication system, where more randomization in secret keys increases the security as well as complexity of the cryptography algorithms. Recently, these algorithms are compensating with enormous memory spaces and large execution time on hardware platform. Field programmable gate arrays (FPGAs), provide one of the major alternative in hardware platform scenario due to its reconfiguration nature, low price and marketing speed. OFDM technique is also being applied in military communications [1].

II. DESIGN METHODOLOGY

A. AES ALGORITHM

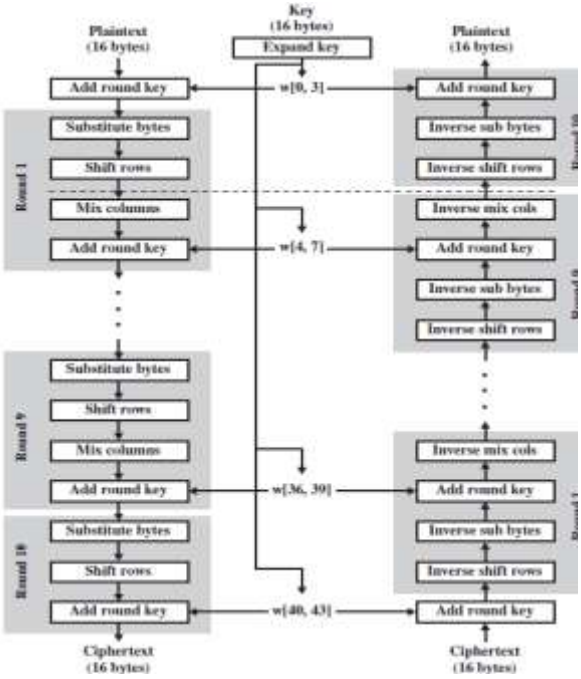
AES is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications. AES operates on 8-bit bytes. Addition of two bytes is defined as the bitwise XOR operation. Multiplication of two bytes is defined as multiplication in the finite field $GF(2^8)$, with the irreducible polynomials $m(x) = x^8 + x^4 + x^3 + x + 1$. The cipher takes a plaintext block size of 128 bits, or 16 bytes. The key length can be 16, 24, or 32 bytes (128, 192, or 256 bits). The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length.

The figure1 shows the AES cipher in more detail, indicating the sequence of transformations in each round and showing the corresponding decryption function.

The following describes the AES structure:

1.The input of encryption and decryption is 128 bits ,considered as single 4x4 matrix plain text.

2. The key that is provided as input is expanded into an array of forty-four 32-bit words, w[i]. Four distinct words (128 bits) serve as a round key for each round.



Encryption **Decryption**

Figure1

3. Four different stages are used, one of permutation and three of substitution:

- Substitute bytes: Uses an S-box to perform a byte-by-byte substitution of the block
- ShiftRows: A simple permutation
- MixColumns: A substitution that makes use of arithmetic over $GF(2^8)$
- AddRoundKey: A simple bitwise XOR of the current block with a portion of the expanded key

4. The structure is quite simple. For both encryption and decryption, the cipher begins with an AddRoundKey stage, followed by nine rounds that each includes all four stages, followed by a tenth round of three stages.

5. Only the AddRoundKey stage makes use of the key. For this reason, the cipher begins and ends with an AddRoundKey stage. Any other stage, applied at the beginning or end, is reversible without knowledge of the key and so would add no security.

6. The AddRoundKey stage is, in effect, a form of Vernam cipher and by itself would not be formidable. The other three stages together provide confusion, diffusion, and nonlinearity, but by themselves would provide no security because they do not use the key. We can view the cipher as alternating operations of XOR encryption (AddRoundKey) of a block, followed by scrambling of the block (the other three stages), followed by XOR encryption, and so on. This scheme is both efficient and highly secure.

7. Each stage is easily reversible. For the Substitute Byte, ShiftRows, and MixColumns stages, an inverse function is used in the decryption algorithm. For the AddRoundKey stage, the inverse is achieved by XORing the same round key to the block, using the result that A(xor)B(xor)B=A .

8. As with most block ciphers, the decryption algorithm makes use of the expanded key in reverse order. However, the decryption algorithm is not identical to the encryption algorithm. This is a consequence of the particular structure of AES.

9. Once it is established that all four stages are reversible, it is easy to verify that decryption does recover the plaintext. Figure1 lays out encryption and decryption going in opposite vertical directions. At each horizontal point (e.g., the dashed line in the figure), **State** is the same for both encryption and decryption.

10. The final round of both encryption and decryption consists of only three stages. Again, this is a consequence of the particular structure of AES and is required to make the cipher reversible.

Therefore ,the decryption plays a reverse operation of encryption to retrieve the original data.[2]

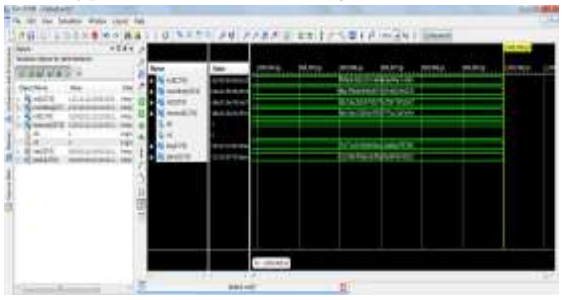


Fig. A

Fig.A shows the simulation of AES Encryption which yields 128 bit ciphertext using 128 bit plaintext and key.

B. OFDM COMMUNICATION SYSTEMS

OFDM allows high data rates transmission for long distances in frequency selective channels as it reduces the effect of Inter Symbol Interference, lSI. Also, OFDM can be used in multi-rate multiplexed channels. The OFDM modulator consists mainly from Serial to Parallel converter, QAM or QPSK, Inverse Fast Fourier Transform, Digital to Analog converter and an optional interleaver. The receiver

consists of an Analog to Digital Converter, FFT, signal mapping, parallel to Serial converter, and an optional de-interleaver

OFDM has been widely used in high speed wireless personal area networks. Also OFDM is used in wireless applications including ETSI DVB-TIH digital terrestrial television transmission and IEEE network standards. However, the design of FFT processors is challenging due to the coexisting requirements of high throughput and accuracy.

In this paper, OFDM comprises of QPSK modulation and IFFT technique in transmitter section whereas in receiver it performs QPSK demodulation and FFT technique.

C. QPSK MODULATION TECHNIQUE

According to this paper, the resultant ciphertext output from aes encryption is fed to the serial to parallel converter where each channel consists of 8-bits,thereby constituting 128 bits(16 channels). Due to orthogonality , each channel permits establishing individual channel data transmission rates which is equal to the channel bandwidth.

QPSK is one of the forms of Phase Shift Keying (PSK) modulation scheme. In QPSK modulation, the carrier phase acquires four discrete states that are used to represent a group of two input data bits as shown in Table 1. Each group takes one form of QPSK states i.e. ±45º and ±135º.

Table 1: QPSK phase with different states

Input	QPSK Phase
00	225º
01	315º
10	135º
11	45º

Where the first bit represents In-phase(I) and the second bit represent the Quadrature-phase(Q). QPSK modulation is a pair of binary PSK [BPSK], but the data transmission in QPSK is twice when compared to BPSK.

The two BPSK waves are added to produce the desired QPSK wave. Since two bit information is transmitted in an interval T, the symbol period for QPSK is two times the bit period i.e. T=2Tb.The QPSK signal requires half the bandwidth of the corresponding BPSK wave which consumes low throughput with complexity in hardware implementation. Hence to generate high throughput QPSK modulator and to verify above statement, hardware implementation is needed. The quadrature-carrier multiplexing system, which produces a modulated wave is described as follows

$S(t) = S_I(t) \cos[2\pi ft] - S_Q(t) \sin[2\pi ft]$

Where $S_I(t)$is the in-phase component, $S_Q(t)$ is the quadrature phase component of the modulated wave. $S_I(t)$ and $S_Q(t)$ is in recognition of the associated cosine or sine versions of the carrier wave, which are in phase-quadrature with each other. Both of these are related to the input data stream in a way that is characteristic of the type of modulation used.

In QPSK, the phase of the carrier takes on one of four equally spaced values, such as $\pi/4$,$3\pi/4$, $5\pi/4$ and $7\pi/4$.

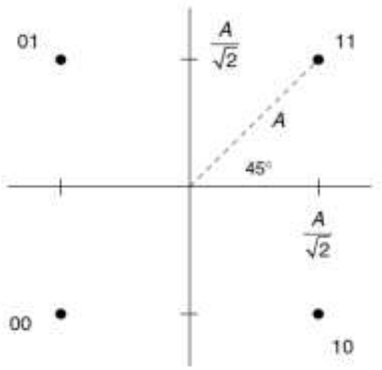


Figure2: Ideal Constellation diagram

When I and Q take on values of $\pm A/\sqrt{2}$ in all possible combinations, the phase of the resulting output signal takes on values of 45, 135, 225, and 315 degrees.

The QPSK demodulation performs the inverse operation at the receiver to get a stream of demodulated data.[3]

D. IFFT AND FFT TECHNIQUE

The modulated output is passed to the IFFT block in order to reduce the number of arithmetic operations from N^2 to NlogN, where N is the size of the FFT. The use of orthogonal carriers makes the output free from ISI(Inter Symbol Interference).

The FFT algorithm eliminates the redundant calculation which is needed in hardware implementation [1]. In addition to computing efficient DFT, computing Discrete Fourier Transform (DFT) and is thus very suitable for efficient

the FFT also finds applications in linear filtering, digital spectral analysis and correlation analysis, Ultra Wide Band (UWB) applications, etc.

In this paper, a pipelined 16-point decimation in frequency (DIF) FFT is implemented by using a Twiddle factor multiplier processor which uses efficient complex twiddle factor multiplication (R+jl) =(X+jY) (C+jS). The Twiddle Factor Wn is represented by 8 bits of which the most significant bit represents the sign of the number and the next bit represents the integer part while the remaining 6 bits represents the decimal part. The twiddle factor represents a sine value or a cosine value. Since the sine or a cosine function varies from –1 to 1, the integer part of the twiddle factor is represented by only 1 bit. Figure 3 describes the implementation of butterfly structure in detail.

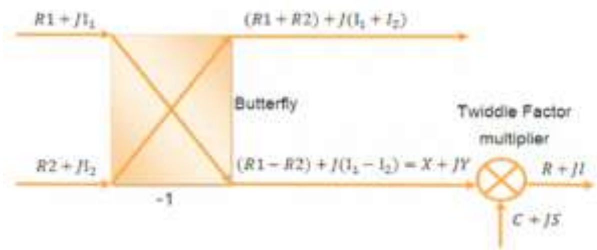


Figure3: The butterfly and its twiddle factor complex multiplier

In figure4 , each stage has four butterflies for both real and imaginary values. Each butterfly consists of upper wing and lower wing. The first stage accepts the input data directly from QPSK mapper which consists of real and imaginary values. The output of first stage is feed as the input to the second stage. The output of second stage is feed as the input to the third stage.The implementation of an 8 Point IFFT processor is done by using components like adders, subtractors, multipliers and buffers[1]. In IFFT the twiddle factor values are of unsigned values which have to be converted into binary form for the multiplication purpose.

In first stage the computation of upper wings is done by using adders and the results are stored in buffers. The computation of lower wings is done by using subtractors and multipliers. Here for every computation of lower wing there is a different twiddle factor which has to be multiplied. After the computation of both upper and lower wings the results are stored in buffers which are fed as input to the second stage.The computation of second stage is also similar to that of first stage but the difference is that for the four lower wings there are only two twiddle factors in common. Here Again the computation results are stored in buffers and are fed to the third stage.

The computation of third stage is also similar to that of first stage but the difference is that there is only one common twiddle factor to be multiplied.

The two 8-point IFFT can be instantiated to attain single 16-point IFFT.

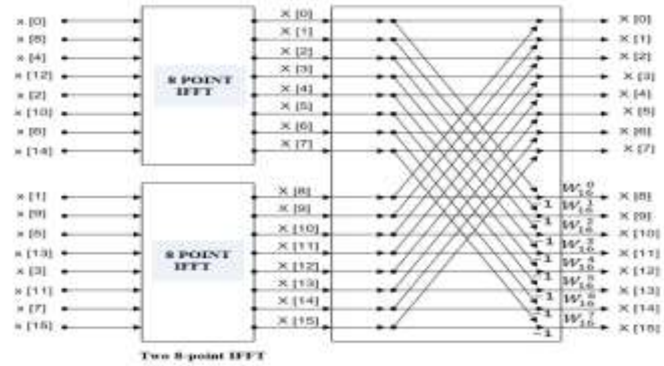


Figure4: Radix-2 DIF_IFFT Flow Graph

The similar rules are to be followed in FFT technique to accomplish the bit reversed output at the receiver section.[4]

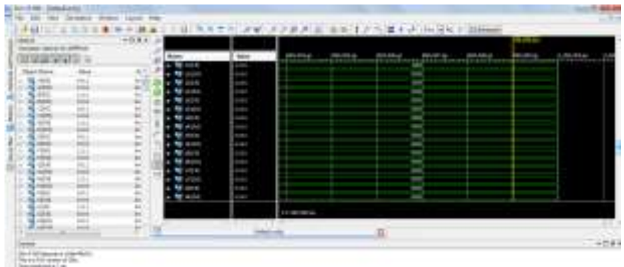


Fig.B

Fig.B shows the simulation of DIF IFFT where the input is in bit reversal sequence and the output in an ordered sequence.

III. CONCLUSION

This paper concludes that especially for military application, it is highly reliable and secured for communication using AES algorithm. It also explores high data rate ,throughput, low fading and interference due to OFDM communication systems. The novelty of this paper is Vedic Mathematics which reduces the complexity in terms of the chips used and power consumption. Even the technical risk can be managed and we get optimum result with the help of this concept.

IV. REFERENCES

1. Ludong Wang, Ph.D. Booz Allen Hamilton, Inc. McLean, VA And Brian Jezek MILSATCOM JTEO McLean, "OFDM Modulation schemes for Military Satellite Communications" MILSATCOM JTEO McLean, Published in Military Communications Conference, IEEE MILCOM 2008 .
2. M.Senthil Kumar, Dr.S.Rajalakshmi," High Efficient Modified Mix Columns in Advanced Encryption Standard using Vedic Multiplier" Published in 2nd International Conference on Current Trends in Engineering and Technology, ICCTET 2014.
3. K.Anitha ,Umesharaddy, B.K.Sujatha," FPGA Implementation of High Throughput Digital QPSK Modulator using Verilog HDL" Published in International Journal of Advanced Computer Research, March-2014.
4. K.Harikrishna, T. Rama Rao, Valadimir A. Labay,"An FFT Approach for Efficient OFDM Communication Systems" , Published in 2010 International Conference on Signal Acquisition and Processing.